UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,398	11/25/2003	Tae Gon Park	8729-227 (IB200306-022)	8075

22150 7590 01/10/2007

F. CHAU & ASSOCIATES, LLC
130 WOODBURY ROAD
WOODBURY, NY 11797

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/721,398	PARK, TAE GON	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17 and 26* is/are rejected.

7)☒ Claim(s) *18-25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Thanhnga B. Truong AU2135

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the communication filed on November 25, 2003. Claims 1-26 are pending. At this time, claims 1-17, and 26 are rejected.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority based on an application filed on November 25, 2003. It is noted, however, that applicant has not filed a certified copy of the instant application as required by 35 U.S.C. 119(b).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-15 are rejected under 35 U.S.C. 102(b) as being anticipated by Hashimoto (US 54,907,275).

a. *Referring to claim 1:*

i. Hashimoto teaches a method for encrypting data (column 3, lines 17-30 of Hashimoto), comprising the steps of:

(1) reading a plaintext data block from a memory **(column 2, lines 20-21 and lines 26-27; column 3, lines 57-60 of Hashimoto);**

(2) storing the plaintext data block in an input buffer **(column 2, lines 22-30 of Hashimoto);**

(3) encrypting the plaintext data block in the input buffer using a first mode to generate a first ciphertext (e.g., encrypted text) **(column 3, lines 16-30 and column 1, lines 19-21 of Hashimoto);**

(4) storing the first ciphertext (e.g., encrypted text) in an output buffer **(column 5, lines 21-23 of Hashimoto)**; and

(5) encrypting the plaintext data block in the input buffer using a second mode to generate a second ciphertext **(column 3, lines 16-30 and column 5, lines 58-64 of Hashimoto)**.

b. *Referring to claim 2:*

i. Hashimoto further teaches:

(1) wherein encryption is performed using CCM **(column 1, lines 19-31 of Hashimoto)**.

c. *Referring to claim 3:*

i. Hashimoto further teaches:

(1) wherein the first mode comprises a CTR (counter) mode **(column 7, lines 45-50 of Hashimoto)**.

d. *Referring to claim 4:*

i. Hashimoto further teaches:

(1) wherein the second mode comprises a CBC (cipher block chaining) mode **(column 1, lines 28-33 and column 7, lines 42-45 of Hashimoto)**.

e. *Referring to claims 5, 9:*

i. Hashimoto further teaches:

(1) further comprising the step of storing the second ciphertext in an initialization vector buffer **(column 7, lines 45-49 of Hashimoto)**.

f. *Referring to claims 6, 10:*

i. Hashimoto further teaches:

(1) further comprising the step of storing the second ciphertext in the output buffer **(column 5, lines 21-23 of Hashimoto)**.

g. *Referring to claim 7:*

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

h. *Referring to claim 8:*

i. This claim has limitations that is similar to those of claims 2-4, thus it is rejected with the same rationale applied against claims 2-4 above.

i. *Referring to claim 11:*

i. Hashimoto teaches a method for decrypting data (column 1, lines 52-58 of Hashimoto), comprising the steps of:

(1) reading a ciphertext (e.g., encrypted text) data block from a memory; storing the ciphertext (e.g., encrypted text) data block in an input buffer; decrypting the ciphertext (e.g., encrypted text) data block in the input buffer using a first mode to generate a plaintext;storing the plaintext in the input buffer, an output buffer or both; and encrypting the plaintext in the input buffer or the output buffer using a second mode to generate a ciphertext **(column 1, lines 49-58 of Hashimoto)**.

j. *Referring to claim 12:*

i. Hashimoto further teaches:

(1) further comprising converting one or more bits of the plaintext to logic level "0" before encrypting the plaintext using the second mode **(column 3, lines 50-51 of Hashimoto)**.

k. *Referring to claim 13:*

i. This claim consist a cryptographic system to implement claim 1, thus it is rejected with the same rationale applied against claim 1 above.

l. *Referring to claim 14:*

i. This claim consist a cryptographic system to implement claim 11, thus it is rejected with the same rationale applied against claim 11 above.

m. *Referring to claim 15:*

i. This claim consist a program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting data to implement claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 16-17 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hashimoto (US 54,907,275), and further in view of Matchett (US 7,092,525).

a. *Referring to claim 16:*

i. Hashimoto teaches a cryptographic apparatus (column 3, lines 17-30 of Hashimoto), comprising:

(1) a memory controller that reads a block of data from a memory **(column 2, lines 18-20 of Hashimoto)**;

(2) an input buffer that stores a block of data read from the memory **(see Figure 2B, element 14 and column 2, lines 22-30 of Hashimoto);**

(3) an encryption module that encrypts the block of data stored in the input buffer using one of a plurality of modes of operation supported by the encryption module including a CTR (counter) mode, CBC (cipher block chaining) mode and CCM (CTR and CBC-MAC (message authentication code) mode (see Figure 1, element 4 and Figure 2B, element 15 and **(column 3, lines 16-30; column 1, lines 19-21; and column 5, lines 58-64 of Hashimoto);**

(4) an output buffer that stores the data encrypted by the encryption module **(see Figure 2B, element 16 and column 5, lines 21-23 of Hashimoto);** and

(5) a control unit that generates control signals to control the memory controller, the input and output buffers and the block encryption module, wherein the control signals comprise a mode control signal that specifies a mode of operation of the encryption module **(column 6, lines 7-22 of Hashimoto).**

ii. Although Hashimoto teaches the encryption systems, Hashimoto is silent on the capability of using a plurality of modes of operation in the encryption system. On the other hand, Matchett teaches:

(1) The use of the DES as a cryptographic system is built around its most basic mode, which is known as the Electronic Code Book (ECB) mode. Other modes of DES, such as Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB), are described in the Federal Information Processing Standards Publication (FIPS PUB) number 81. In the ECB mode, a 64-bit plaintext word is converted to a 64-bit ciphertext word. This conversion is a one-to one and reverse mapping is electable. This conversion is also done under the control of a 56-bit keying variable. The keying variable for the DES is generally given as 64-bits with the convention of using 8 bits as the odd parity bits. Alternative Modes of Using the DES from FIPS PUB 81, DES Modes of Operation are the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode. ECB is a direct application of the DES algorithm to encrypt and decrypt data; CBC is an enhanced mode of ECB which chains together blocks of cipher text; CFB uses previously generated cipher text as input to the DES to generate pseudorandom outputs which are combined with the plaintext to produce cipher, thereby chaining together the resulting cipher; OFB is identical to CFB except that the previous output of the DES is used as input in OFB while the previous cipher is used as input in CFB. OFB does not chain the cipher **(column 1, lines 30-51).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Hashimoto with the teaching of Matchett to an improved Data Encryption Standard (DES) cryptographic system for cryptographic protection of data through modifications to the cipher function and cipher key as specified in the DES **(column 1, lines 13-16 of Matchett).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Hashimoto with the teaching of Matchett to provide an enhanced DES cryptographic system having an enhanced DES device and process to strengthen the cryptanalytic resistive structure of the DES **(column 4, lines 16-18 of Matchett).**

b. *Referring to claim 17:*

i. Hashimoto further teaches:

(1) wherein the encryption module comprises: a PL (preload) register that stores data associated with a CTR mode; an adder module that adds a logic "1" to data output from the PL register ; an IV (initialization vector) register that stores data associated with a CBC mode; a data input register that stores an data block input from the input buffer; a data output register that stores a data block to be output to the data output buffer; a first logic operator that performs an exclusive-or (XOR) operation on data in the IV register and the data input register; a block cipher module; and a second logic operator that performs an XOR operation on data output from the block cipher module and data in the input register **(see Figure 1 of Hashimoto and more details in column 3, lines 32-67 through column 4, lines 1-2).**

c. *Referring to claim 26:*

i. Hashimoto teaches

(1) A communications system (e.g., network) **(column 4, lines 64-67 of Matchett)** comprising the cryptographic apparatus of claim 16.

Allowable Subject Matter

7. Claims 18-25 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. McGrew (US 7, 095, 850 B1) discloses an encryption method and apparatus that provides forward secrecy, by updating the key using a one-way function after each encryption. By providing forward secrecy within a cipher, rather than through a key management system, forward secrecy may be added to cryptographic systems and protocols by using the cipher within an existing framework (see abstract).

b. Kaplan et al (US 6,704,871 B1) discloses a secure communication platform on an integrated circuit is a highly integrated security processor which incorporates a general purpose digital signal processor (DSP), along with a number of

high performance cryptographic function elements, as well as a PCI and PCMCIA interface (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
January 3, 2007

Thanhnga B. Truong
AU2135